Probabilistic Admissible Encoding on Elliptic Curves - Towards PACE with Generalized Integrated Mapping

Łukasz Krzywiecki, Przemysław Kubiak,
Mirosław Kutyłowski

Wrocław University of Technology, Poland

SOFSEM 2014, Novy Smokovec

Talk Agenda

1. password authentication and personal ID documents
2. patents
3. escaping the patents

Password authentication

Personal ID documents with wireless interface

1. a smart card is a slave: responds to commands from the reader
2. the owner might be unaware that an interaction takes place
3. but: the smart card has a state automaton and responds to the reader according to the security status
4. e.g. a command with the correct PIN necessary to execute a signing command

Password authentication

Outline

1. the password either entered by the document owner to the reader via keyboard or read optically from the card surface (Card Access Number)
2. in order to cooperate with the reader **the smart card must get convinced that the reader knows the correct password**
3. an eavesdropper can monitor the radio channel

Requirements

1. a malicious reader may initiate the protocol and try one password
2. it must be impossible to try more than one password per session – in particular with offline cryptanalysis afterwards
3. the malicious reader may play all tricks – in particular not behave according to the protocol
4. even the smart card identity should be hidden from the eavesdropper

PACE
design outline

Password Authenticated Connection Establishment

1. designed to be patent free (elegant SPEKE protocol from the US is good but covered by a patent)
2. designed by German authority BSI for *Machine Readable Travel Documents*
3. adopted by ICAO - the facto standardization authority for travel documents
4. password authentication planned to be introduced in EU

PACE

password dependent data

Card		Reader
π installed		π input by the owner
$K_\pi := H(0\Vert\pi)$		$K_\pi := H(0\Vert\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if $Y_B \not\in \langle g \rangle \setminus \{1\}$		abort if $Y_A \not\in \langle g \rangle \setminus \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{\ldots} := H(\ldots\Vert K)$		$K_{\ldots} := H(\ldots\Vert K)$

PACE

first DH key exchange - base establishment

Card		Reader
π installed		π input by the owner
$K_\pi := H(0\Vert\pi)$		$K_\pi := H(0\Vert\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G},z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g\rangle\setminus\{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g\rangle\setminus\{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
check $Y'_B \neq Y_B$	$\xrightarrow{Y'_A}$	check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{\dots} := H(\dots\Vert K)$		$K_{\dots} := H(\dots\Vert K)$

PACE

first DH key exchange - base establishment

Card		Reader
...		...
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
...		...

- definition of $\hat{g}$ is so called **Generic Mapping** - PACE v1 Generic Mapping (PACE-GM). according to *ISO/IEC JTC1 SC17 WG3/TF5 for the International Civil Aviation Organization: Supple- mental access control for machine readable travel documents (2011)*
- Integrated Mapping (PACE-IM) from the same standard – specific operations for ECC, partially patented.

PACE

the second Diffie-Hellman for key establishment

Card		Reader
π x_A, $X_A = g^{x_A}$		π
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
check $Y'_B \neq Y_B$	$\xrightarrow{Y'_A}$	check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{...} := H(...\|\|K)$		$K_{...} := H(...\|\|K)$

PACE

final phase - proof of possession and deriving keys

Card		Reader
$\dots$		$\dots$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{ENC} := H(1 \Vert K)$		$K_{ENC} := H(1 \Vert K)$
$K_{MAC} := H(2 \Vert K)$		$K_{MAC} := H(2 \Vert K)$
$K'_{MAC} := H(3 \Vert K)$		$K'_{MAC} := H(3 \Vert K)$
$T_A :=$ $MAC(K'_{MAC}, (Y'_B, \mathcal{G}))$		$T_B :=$ $MAC(K'_{MAC}, (Y'_A, \mathcal{G}))$
	$\xleftarrow{T_B}$	
abort if T_B invalid		
	$\xrightarrow{T_A}$	
		abort if T_A invalid

- the chip interrupts if it discovers that the tag of the reader is wrong,
- until this moment **all data sent to the reader by the chip have the uniform probability distribution for every password** ...
- ... and for **every choice of the reader**

PACE

final phase - proof of possession and deriving keys

Card		Reader
$\dots$		$\dots$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{ENC} := H(1 \vert\vert K)$		$K_{ENC} := H(1 \vert\vert K)$
$K_{MAC} := H(2 \vert\vert K)$		$K_{MAC} := H(2 \vert\vert K)$
$K'_{MAC} := H(3 \vert\vert K)$		$K'_{MAC} := H(3 \vert\vert K)$
$T_A := MAC(K'_{MAC}, (Y'_B, \mathcal{G}))$		$T_B := MAC(K'_{MAC}, (Y'_A, \mathcal{G}))$
	$\xleftarrow{T_B}$	
abort if T_B invalid		
	$\xrightarrow{T_A}$	
		abort if T_A invalid

- the reader interrupts if it discovers that the tag of the chip is wrong (maybe the communication was hijacked by another device?)
- until this moment **the reader sent one message that depends on password**

Integrated mapping

Integrated mapping

Find a way to map the password and parameters exchanged via the radio channel to a point of an elliptic curve.
It should have the similar properties as for SPEKE (the element $(H(parameters, \pi))^2$) or PACE GM (described above)

Why we need integrated mapping?

1. DH group implemented as Elliptic Curve on the smart card, so the EC implementation is already there
2. direct tailored mapping can improve efficiency

Security status

Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping
Jean-Sebastien Coron, Aline Gouget, Thomas Icart, and Pascal Paillier
Cryptography and Security: From Theory to Applications LNCS 6805, 2012, pp 207-232

Integrated Mapping

Card		Reader
π		π
	RANDOMIZATION	
choose $s \leftarrow \{0,1\}^{l_1}$ $z := ENC(K_\pi, s)$		
	$\xrightarrow{z}$	
		$s := DEC(K_\pi, z)$
	MAPPING	
		choose $\beta \leftarrow \{0,1\}^{l_2}$
	$\xleftarrow{\beta}$	
$\hat{G} := Encoding(H(s, \beta))$		$\hat{G} := Encoding(H(s, \beta))$
	PROCEED WITH THE REST OF PACE	
	...	

Integrated mapping

legal situation

From paper“ Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping”:

- “PACE v2 IM relies on a cryptographic method (Icart’s point encoding) owned by Sagem Sécurité. However Sagem Sécurité has agreed to grant free-of-charge exploitation rights under **restrictive conditions**” [1].
- bibliography position [1]: Patent Statement and Licensing Declaration Form for ITU-T/ITU-R Recommendation ISO/IEC Deliverable. Letter from Sagem Sécurité to ICAO New Technologies Working Group International Civil Aviation Organization, Paris, May 04th 2010.
- “Alternatively PACE v2 IM can use the simplified SWU encoding function into elliptic-curve” (see **EP 2527970 A1** below)

Integrated mapping
legal situation

Issues

- what about the general use? The letter from Sagem was directed to ICAO and not as a general unlimited waiver of rights.
- In many legal systems the declaration **must define** the recipient of rights.

Importance

- the stack of protocols developed for personal ID cards **could be re-used** for many purposes, e.g. sensor networks
- positive side: cryptographic strength, privacy by design, libraries, implementations on smart cards, price
- negative side: would you dare to take the legal risk to design systems based on (possibly) patented mathematics?

Patents

main goals (theory)

1. protect inventor’s intellectual rights
2. protect the right of the inventor to make a reasonable profit
3. prevent blocking a justified use of the invention.

Patents

main goals (theory)

1. protect inventor's intellectual rights
2. protect the right of the inventor to make a reasonable profit
3. prevent blocking a justified use of the invention.

implementation

1. 20 years monopoly for the inventor (conditioned by the payment of the fees)
2. it does not matter who made an invention, who applies first gets the exclusive rights
3. win-win system for the patent authority

European Patent Convention

5 Oct 1973

Article 52, patentable inventions

(1) European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

(2) The following in particular **shall not be regarded as inventions within the meaning of paragraph 1**:

(a) discoveries, scientific theories and **mathematical methods**;

(b) aesthetic creations;

(c) schemes, rules and methods for performing mental acts, playing games or doing business, and **programs for computers**;

(d) presentations of information.

European Patent Convention

5 Oct 1973

Article 52, Patentable inventions

(3) Paragraph 2 **shall exclude the patentability** of the subject-matter or activities referred to therein **only to the extent** to which a European patent application or European patent relates **to such subject-matter or activities as such.**

(3) Absatz 2 steht der Patentierbarkeit der dort genannten Gegenstände oder Tätigkeiten nur insoweit entgegen, als sich die europäische Patentanmeldung oder das europäische Patent auf diese Gegenstände oder Tätigkeiten als solche bezieht.

(3) Le paragraphe 2 n'exclut la brevetabilitédes éléments qu'il énumère que dans la mesure où la demande de brevet européen ou le brevet européen concerne l'un de ces éléments, considéréen tant que tel.

Myths

“mathematics cannot be patented in Europe”

- Ok, mathematics as such cannot be patented.
- On the other hand, one can get a patent for a mathematical method (algorithm) used on hardware for for a specific purpose.
- Almost all crypto computations require devices, the usage goals might be very general.

- E.g. Diffie-Hellman key exchange could have been patented in Europe.

Myths

“computer programs cannot be patented in Europe”

- Ok, a computer program as such cannot be patented.
- On the other hand, one can get a patent on program idea (algorithm).
- Additionally, the program as such is protected by the copyright.
- The copyright protection is even harder (protection period is 70 years) and no fees apply.

- Put a source code on a web kills all **legal** possibilities to reuse the code without explicit permission of the author.
- The copyright owner can just wait until you collect enough money via violating the copyright to his code.

Example

Method for cryptographic encoding on an elliptic curve

EP 2527970 A1, Abstract

The method involves determining a point belonging to an elliptical curve defined on a finite characteristic body, and executing a simplified Shallue-Woestijne-Ulas (SWU) encoding function from an element shared between devices (101, 102) by execution units (111, 112). The function is executed by one of the devices by using a representation system i.e. Jacobean representation system, of coordinates of points, where the system is different from affine representation system of coordinates of points. A correction step is performed for obtaining an equivalent point identical between the devices. Independent claims are also included for the following: (1) a computer program product comprising program code instructions for implementing a method for executing a portion of cryptographic calculation (2) a non-transitory computer-readable storage medium storing a computer program that comprises program code instructions for implementing a method for executing a portion of cryptographic calculation (3) a device comprising units for implementing a method for executing a portion of cryptographic calculation.

Example

Method for cryptographic encoding on an elliptic curve

EP 2527970 A1, Abstract

The **method** involves **determining a point belonging to an elliptical curve** defined on a finite characteristic body, and executing **a simplified Shallue-Woestijne-Ulas (SWU)** encoding function from an element shared between **devices** (101, 102) by execution units (111, 112). The function is executed by one of the devices by using a representation system i.e. Jacobean representation system, of coordinates of points, where the system is different from affine representation system of coordinates of points. A correction step is performed for obtaining an equivalent point identical between the devices. Independent claims are also included for the following: (1) **a computer program product comprising program code instructions for implementing** a method for executing a portion of cryptographic calculation (2) **a non-transitory computer-readable storage medium storing** a computer program that comprises program code instructions for implementing a method for executing a portion of cryptographic calculation (3) **a device comprising units for implementing** a method for executing a portion of **cryptographic calculation**.

Polish patent law

Art. 28.

Za wynalazki, w rozumieniu art. 24, nie uważa się w szczególności:

1) odkryć, teorii naukowych i metod matematycznych;

2) wytworów o charakterze jedynie estetycznym;
3) planów, zasad i metod dotyczących działalności umysłowej lub gospodarczej oraz gier;
4) wytworów, których niemożliwość wykorzystania może być wykazana w świetle powszechnie przyjętych i uznanych zasad nauki;
5) programów do maszyn cyfrowych;
6) przedstawienia informacji.

Polish patent law

Art. 28.

Za wynalazki, w rozumieniu art. 24, nie uważa się w szczególności:
Within the meaning of Art. 24, the following categories are not considered as inventions:
1) odkryć, teorii naukowych i metod matematycznych; **scientific discoveries, scientific theories and mathematical methods**
2) wytworów o charakterze jedynie estetycznym;
3) planów, zasad i metod dotyczących działalności umysłowej lub gospodarczej oraz gier;
4) wytworów, których niemożliwość wykorzystania może być wykazana w świetle powszechnie przyjętych i uznanych zasad nauki;
5) programów do maszyn cyfrowych; **computer programs**
6) przedstawienia informacji.

no rule limiting the scope of article 28 to “methods and objects as such”

Other countries

Germany

“... steht der Patentfähigkeit nur insoweit entgegen, als für die genannten Gegenstände oder Tätigkeiten als **solche Schutz** begehrt wird.”

Slovakia

“(4) Predmety alebo činnosti uvedené v odseku 3 sa vylučujú z patentovatelnosti len v rozsahu, v akom sa prihláška vztahuje na tieto predmety alebo činnosti.”

EP 2527970 A1

a part of the invention description

The implementation of the SWU simplified encoding function to derive a point from an affine element coordinates *u* comprises the following successive steps:

a) $\alpha = -u^2$ mod p

b) $X_2 = -b((1 + \alpha + \alpha^2)/(a(\alpha + \alpha^2)))$ mod p

c) $X_3 = \alpha X_2$ mod p

d) $H_2 = (X_2)^3 + aX_2 + b$ mod p

e) $h_3 = (X_3)^3 + aX_3 + b$ mod p

f) $U = u^3 h_2$ mod p

g) $A = (h_2)^{p-1-(p+1)/4}$ mod p

h) if $A_2 h_2 = 1$ mod p, then $(x, y) = (X_2, Ah_2$ mod $p)$

i) else $(x, y) = (X_3, AU$ mod $p)$

Patents in Europe

resulting situation

lesson to be learnt:

- **you are free to make research**: develop theory, design algorithms, develop products . . .
  . . . **as long as they are not used in practice** for commercial purposes
- **going to applications is risky** – it may turn out that you violate the patents and you have to **pay** somebody for the product that you have designed yourself
- if you wish to play the game **you need professional support from law specialists**

Patent aware research

Traditional research

- collect the *previous work* papers
- start research
- if you improve the *previous work*, then with high probability the result is new and you can protect your copyright to the result

Patent aware research

Traditional research

- collect the *previous work* papers
- start research
- if you improve the *previous work*, then with high probability the result is new and you can protect your copyright to the result

but it can turn out that you violate some patent

Research approach - *technology transfer ready*

- collect the *previous work* papers
- analyze the patents
- start research
- if you improve the *previous work* you can protect your copyright to the result but also **you have to compose a complete list of patents used**

Patent aware research

Understanding a patent description

difficult for the following reasons:

- special language due to legal rules
- patent description for algorithms are not formulated by patent law specialists
- the patents are to protect the owners and not to disseminate ideas
- obfuscation on purpose: make the life hard for the competitors
- ambiguity on purpose: keep doors open for the future claims

Finding the patents

much easier now – many thanks to Google!
but **do you really want to spend months by analyzing the patent claims before you write a single paper?**

Patent tricks

Strategy 1

whatever algorithm idea you have **make a patent application before you get it ready:** stable algorithm description, its correctness proof, efficient implementation, . . .

Strategy 2 (dishonest)

make an application after leaving a seminar room after brainstorming with your colleagues

FIRST IN FIRST SERVED – do it fast, before your colleagues do the same

Patent tricks

Strategy 3 (dishonest)

- Collaborate with the patent office in country A.
- After learning an idea make an application and backdate it.
- A golden period between the application date and the publication date - a year or so.

Strategy 4 (dishonest)

- Collaborate with the patent officer in country A
- When an application is submitted submit the same application (but with your name as the inventor) in country B.
- The officer in country A rejects the application for some formal reason.
- Due to the concept of European patent law you get protection in country A.

Our technical results

Goal: remove specific assumptions from the previous mapping techniques

- escape the specific tailored (patented) versions of the general (patent-free) algorithms, get solutions outside the patent scope
- make it flexible so that one has as much free choice of the parameters as possible
  (some curves might turn out to be insecure, new efficient algorithms/implementations may emerge for some new types of curves, some curves might turn to be patented, . . .

Execution time

threats of information leakage

Time oblivious randomized

- For a smart card an input dependent execution time is a disaster – it may lead to secret information leakage.
- For this reason a deterministic algorithm is an advantage for the system designers and security certification.

However, it is enough that:

- the probability distribution of execution time is exactly the same for each input

Our results

Indistinguishability model

tailoring to the case of time-oblivious algorithms
– every works fine!

A mapping based on general algorithms that

1. is time oblivious with a reasonable upper time bound
2. avoids a few limitations
3. has computation time only slightly increased

Very technical details in the paper

. . .

Remarks concerning smart card implementation

Efficiency

1. the square root algorithm used in the paper needs Jacobi symbol computations,
2. to preserve algorithm's efficiency on smart cards hardware implementation of the Jacobi symbol is needed (the symbol is called inside a loop),
3. luckily, gcd of two integers and Jacobi symbol computations are similar, hence part of the circuits should be useful both for Jacobi symbol and for inverting elements in prime fields,
4. efficient inversion eliminates the need for projective coordinates (affine ones could be used).

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl, Przemyslaw.Kubiak@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl